HISEC 2003

Az informatikai biztonság felügyeleti és tanúsító intézményrendszere

Muha Lajos
információbiztonsági igazgató
Persecutor Vagyonvédelmi Kft.

A modern állam működtetéséhez szükséges nagy tömegű információt a hagyományos módszerekkel egyre kevésbé lehet kezelni. Az államnak általában és az egyes állami szervezeteknek különösen fontos érdeke fűződik ahhoz, hogy *az informatikai rendszerekben feldolgozott adatok bizalmasságát, hitelességét, sértetlenségét és rendelkezésre állását megőrizze*. Az Európai Unióhoz való csatlakozás során ezzel kapcsolatban már követelmények is megjelennek hazánkkal szemben, de, mint NATO tagországgal szemben is vannak elvárások.

Globalizálódó világunkban új fenyegetések jelentek meg. A XXI. század hadszíntere a „cybertér" lett, az információs hadviselés többek között az informatikai rendszerek támadásával, bénításával tervezi a győzelemhez szükséges információs fölényt megszerezni. A számítógépes terrorizmus, részben mint a nemzetközi terrorizmus része, másrészt a számítógépes bűnözésen keresztül is az informatikai rendszerek biztonságát veszélyezteti. Egy esetleges terror-támadás során logikai bombák útján a bank- és tőzsdeszámlák kiürítésre kerülhetnek, a légi irányításban katasztrófákat idézhetnek elő, a távközlési rendszereket túlterheléssel béníthatják meg. Ma hazánkban a közigazgatás, illetve a stratégiai fontosságú szervezetek *informatikai rendszereinek biztonsága a „szabad belátásra" van bízva*, ezért mindenképpen szükségszerű az államilag szabályozott biztonsági követelményeket az informatikai rendszereket felhasználók széles táborára, a közigazgatás szervezeteitől kezdve az állami irányítás alatt álló szervezeteken keresztül a stratégiai feladatokat ellátó szervezetekig kiterjeszteni.

A kormányzaton belül az informatikai rendszerek összekapcsolódásával a biztonság kérdése tovább bonyolódik. Az együttműködő informatikai rendszerek esetében alapkövetelmény, hogy azok biztonsági szempontból egyenszilárdságúak legyenek. Fontos továbbá, hogy az informatikai rendszerek felhasználói minden körülmények között megbízzanak az általuk használt rendszer védettségében, biztonságában.

Az informatikai rendszerek előállítói, vagy árusítói garantálnak bizonyos biztonsági (védettségi) szintet, illetve azokat a felhasználók részben maguk is megismerhetik, mégis cél-

szerűbb **nemzetközileg elfogadott követelmények alapján lefolytatott vizsgálati eredményekre támaszkodni**. A rendszereknek vagy termékeknek az értékeléséhez objektív és jól körülhatárolt biztonsági követelményrendszeren túl egy **olyan testület létezésére is szükség van, mely garantálja, hogy a vizsgálatot megfelelő módon hajtották végre**.

Egy nemzeti, informatikai biztonság hatóság létrehozásának szükségességét alátámasztja az is, hogy az Európa Tanács Távközlési és Információs Társadalom Munkacsoportja tárgyalásokat folytat egy központi informatikai biztonsági szervezet, az „European Network and Information Security Agency" (ENISA) létrehozásáról, amely a nemzeti hatóságok tevékenységet nem érinti, illetve bizonyos területeken azt összehangolni hivatott. Ennek a szervezetnek a keretei, feladatai ma még kialakítás alatt vannak, de szinte bizonyos, hogy létrehozásra kerül.

Ma még hazánkban gyakorlatilag hiányoznak az informatika szerepének, illetve az informatikai rendszerek veszélyeztetettségének megfelelő, **az informatikai biztonságra vonatkozó jogi keretek**, amelyek nélkülözhetetlenek az informatikai biztonság kormányzati szintű koordinációjához, hatékony megvalósításához.

1992-98 között a *Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága* nemzetközi, elsősorban Európai Uniós alapokon nyugvó ajánlásokat adott ki. Az 1994-ben kiadott 8. számú (Informatikai biztonsági módszertani kézikönyv), az 1996-ban kiadott 12. számú (Az Informatikai Rendszerek Biztonsági Követelményei), továbbá az 1998-ban kiadott 16. számú (Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana) ajánlása az informatikai biztonság témakörében ismert és használt ajánlásokká váltak. Az 1996-ban elkészült, állami feladatokat is megszabó „Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve" című tanulmány már nem került kiadásra. 1998 után a nemzetközi ajánlások, szabványok nem kerültek ezen a téren honosításra, feldolgozásra.

Az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény 30. § (2) bekezdése ugyan előírta, hogy „a Kormány - az érintett állami szervek vezetőivel egyetértésben - a minősített adatot kezelő információs rendszerek létesítésének és működésének rendjét 1995. december 31-ig határozza meg", azonban, bár ennek a Miniszterelnöki Hivatal Informatikai Koordinációs Iroda több változatát elkészítette – nem sikerült a tárcaközi egyeztetéseken átvinni. A törvény 25.§ (1) bekezdés szerint "a minősített adatok védelmének szakmai felügyeletét a belügyminiszter látja el, a honvédségnél, valamint a polgári nemzetbiztonsági szolgálatoknál - e jogkörét a hatáskörrel rendelkező miniszterrel együttesen gyakorolja". A törvény

2003. évi módosítása (2003. évi LXXX (VI.23.) törvény az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény, valamint az azzal összefüggésben más törvények módosításáról) bevezeti a négyfokozatú minősítésű rendszert, ezzel egyrészt megvalósította a magyar minősítési rendszer NATO, EU, EURATOM és NYEU harmonizációs célú átalakítását, megszüntette a még meglevő minősítési automatizmusokat.

A törvény alapján a belügyminiszter 2003-ban (!) ajánlást adott ki a minősített adatok kezeléséről és védelméről, a minősítési hatáskör jogszerű gyakorlásáról és a titokvédelmi rendszer alkalmasságának vizsgálatáról [Belügyi Közlöny XIV. évfolyam 1. szám.] foglalkozik a titokvédelmi alkalmasság vizsgálatával, és ezen belül a kommunikációs és informatikai biztonsággal.

A Nemzeti Biztonsági Felügyeletről szóló módosított 1998. évi LXXXV. törvény 1. § (1) szerint „A Nemzeti Biztonsági Felügyelet (a továbbiakban: Felügyelet) az Észak-atlanti Szerződés Szervezete (a továbbiakban: NATO), a Nyugat-európai Unió (a továbbiakban: NYEU), az Európai Unió Tanácsa és az Európai Bizottság, valamint az EURATOM (a továbbiakban együtt: EU) Biztonsági Szabályzataiban előírt követelmények érvényesítéséért felelős, a Miniszterelnöki Hivatal szervezeti keretében működő, önálló feladattal és hatósági jogkörrel rendelkező szervezet.”.

A 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról 4.§ h) alapján az Információs Hivatal ellátja a rejtjeltevékenység szakirányítását, hatósági engedélyezését, felügyeletét, és rejtjelkulcsot állít elő. A 43/1994. (III.29.) Kormányrendelet a rejtjeltevékenység szakirányításának, hatósági engedélyezésének és felügyeletének részletes szabályait rendezi.

Az elektronikus aláírásról szóló 2001. évi XXXV. törvényben, illetve a kapcsolódó rendeletekben (15/2001. (VIII. 27.) MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról, 16/2001. (IX.1.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről, 2/2002. (IV.26.) MeHVM irányelv a minősített elektronikus aláírásokkal kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről) a biztonság kérdései kizárólag az elektronikus aláírásra korlátozódnak. Az elektronikus aláírásról rendelkező törvény az európai uniós ajánlásban foglaltaknak megfelelően megteremti a jogszabályi kereteket az állam- és közigazgatásban és az információs társadalom által érintett más területeken az elektronikus aláírás széleskörű, kötelező érvénnyel elismert használatához. A törvény bevezeti a különböző szintű biztonságot megvalósító eszközrendszer használatát feltételező fokozott és minősített aláírás fogalmát, mely

utóbbi lehetővé teszi a papír alapú dokumentum kézi aláírásával egyenértékű elektronikus okirat használatát. Azonban a (matematikai és informatikai szempontból) szorosan idetartozó és ma már a civil szférában általános használt, de a NATO-ban is követelményként jelentkező nyilvános kulcsú rejtjelzés kérdései sem kerültek szabályozásra. Az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 17. § a) pontja felhatalmazta a Miniszterelnöki Hivatalt vezető minisztert, hogy az érintett miniszterekkel egyetértésben, rendeletben szabályozza az informatikai biztonság követelményeit, de ezen a téren sem történt érdemi előrelépés.

A vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról szóló 1998. évi IV. törvény szerint, míg a bármilyen őrző-védő tevékenység engedély köteles, addig az üzleti és üzemi titok, valamint az informatikai adatok védelme, mint a személy- és vagyonvédelemmel, illetve a magánnyomozással közvetlenül összefüggő, külön engedély nélkül végezhető tevékenység került meghatározásra.

A jogszabályokon túl egyéb, nemzetközi kötelezettségekből adódó követelményeket is figyelembe veszünk a munkánk során. Ilyen, pl. a Számítástechnikai bűnözés elleni egyezmény, melyet 47 állam írt alá Budapesten 2001. november 23-án. Az egyezmény alapvető célja "közös büntetőjogi politika kialakítása, a társadalom védelmének biztosítása a számítástechnikai bűnözéssel szemben, többek között megfelelő jogszabályok elfogadásával és a nemzetközi együttműködés elősegítésével". A nemzetközi egyezmény megszületését egyre szaporodó és egyre veszélyesebb "számítógépes bűncselekmények" (a számítógépes csalás, a szerzői jogok megsértése, a gyermekpornográfia terjesztése, a számítógépes hálózatok biztonsága elleni cselekmények) és ezeknek az egyes országok fizikai és saját igazságszolgáltatási határait egyaránt túllépő jellege indokolta. Az Egyezmény nyomán a magyar büntetőjog, illetve a Büntető Törvénykönyv az alábbi tényállásokat kezeli számítógépes bűncselekményekként (számítógépes bűnözésként):

- 300/C. §. Számítástechnikai rendszer és adatok elleni bűncselekmény,
- 300/E. §. Számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása,
- 312/B. §. Fedezetlen bankkártya felhasználása,
- 313/B. §. Bankkártya-hamisítás,
- 313/C. §. Bankkártyával visszaélés,
- 329/A. §. Szerzői vagy szerzői joghoz kapcsolódó jogok megsértése,

- 329/B. §. Szerzői vagy szerzői joghoz kapcsolódó jogok védelmét biztosító műszaki intézkedés kijátszása és
- 329/C. §. Jogkezelési adat meghamisítása.

A PECA egyezmény (Protocol on European Conformity Assessment) az egyezményben hazánk vállalta, hogy az EU-s (CEN, CENELEC és ETSI) szabványokat elfogadjuk, tanúsító szervezeteket jelölünk ki, és jelentünk be az EU-nak. Ebből kettő, a LVD és az EMC direktívák) közvetve érinti az informatikai biztonságot is. A PECA egyezmény alapján a MEEI és a TÜV bejelentett (vagyis az egyezmény keretében bejelentett [notified] és az EU hivatalos lapjában is közzétett) vizsgálati és tanúsító szervezet, így vizsgálati eredményeit és tanúsítványait az EU tagállamok is elfogadják.

A korábban is meglévő elmaradásunk ezekkel a jogalkotási és szabványosítási hiányosságokkal immár több évtizedesnek tekinthető. Az informatikai biztonság területén a szabályozottság hiányában megjelentek azok a „kóklerek", akik felületes szakmai ismeretekkel, vevőiket megtévesztve végeznek informatikai biztonsági átvilágításokat, kockázatelemzéseket, készítenek különböző szabályzatokat, tartanak oktatásokat, továbbképzéseket. Ezzel a „digitális szakadék" tovább mélyül, az ilyen szolgáltatást igénybevevőknél hamis biztonságtudat alakult ki.

Az elmúlt egy évben a kérdéskör újra felszínre került. A Magyar Köztársaság nemzeti biztonsági stratégiájáról szóló 2144/2002. (V. 6.) kormányhatározat melléklete (Biztonság az új évezred küszöbén) szerint „*Magyarország érdeke ... (az informatikai és telekommunikációs) rendszerek védelme ...*".

A Magyar Információs Társadalom Stratégia készítéséről, a további feladatok ütemezéséről és tárcaközi bizottság létrehozásáról szóló 1214/2002. (XII. 28.) kormányhatározat előírja, hogy 2003. október 15-ig „*a valamennyi stratégiai területen jelentkező közös feladatok megoldását alapjaiban érintő legfontosabb technológiai problémák kezelése érdekében, a stratégia kidolgozásával párhuzamosan ... ki kell alakítani, az informatikai alkalmazások minőségének és biztonságának hiteles tanúsítási rendjét, az ehhez szükséges jogszabályok megalkotásával és intézményrendszer felállításával.*"

A 2004-ben várható EU csatlakozásunkig a szervezeti rendszer összhangját is meg kell teremteni azért, hogy az EU szervezeteihez történő csatlakozás és a kapcsolattartás is megoldható legyen. A legtöbb fejlett informatikai szinten álló európai országban létezik ún. InfoSec hatóság. A legtöbb fejlett országban az informatikai biztonságot egy központi kor-

mányszerv (hatóság vagy hivatal) fogja össze (pl. UK: CESG, Németország: BSI, Franciaország: DCSSI, USA: NSA és NIST).

Magyarországon ma nincs központi felügyelet, irányítás. Több szervezet felelős a különböző részterületekért, és ezek döntő többsége is csak a minősített információk védelmére irányul, ezért maradnak lefedetlen részterületek.

A fentieket is figyelembe véve hazánkban is létre kell hozni egy olyan, a Kormány irányítása alatt működő, törvényben vagy kormányrendeletben hatáskörébe utalt feladatokat végző, a piaci szereplőktől független, országos illetékességű, hatósági jogkörrel és jogi személyiséggel rendelkező központi közigazgatási szervezet (a továbbiakban: Felügyelet) létrehozásáról, amely az informatikai biztonsági feladatokat az Európai Uniós és a NATO elvárásoknak is megfelelő szinten képes ellátni.

Elsősorban az Európai Unió elvárásait, illetve az uniós államokban már működő szervezetek feladatait figyelembe véve a Felügyelet feladatait a következőkben foglalhatjuk összse:

(1) gondoskodik az informatikai rendszerek és eszközök – és különösen a minősített adatot kezelő informatikai rendszerek – biztonsági követelményeinek, szabványainak és ajánlásainak kidolgozásáról (honosításáról) és karbantartásáról;
(2) közvetíti az állami irányítás alatt álló és a stratégiai feladatokat ellátó szervezeteknek az informatikai rendszerek biztonsági követelményeit, útmutatást, valamint segítséget nyújt ezek értelmezésében és végrehajtásában,
(3) ellátja az informatikai eszközök (termékek) – az Országos Rejtjelfelügyelet hatáskörébe tartozó eszközök kivételével – informatikai biztonsági tanúsításának felügyeletét, a tanúsítás alapján kiadja az informatikai rendszerek és eszközök informatikai biztonsági minősítését;
(4) ellátja az informatikai rendszerek vagy eszközök biztonsági vizsgálatát végző személyek és szervezetek működésének engedélyezését és felügyeletét[1];

[1] a) Az informatikai termékek biztonsági tanúsítása és minősítése a jelenleg nemzetközileg elfogadott ISO 15408 szabvány szerint kell, hogy történjen. Ehhez elengedhetetlen a „Common Criteria” egyezményhez való csatlakozásunk

b) Ennek a szervezetnek a feladata kell, hogy legyen a TEMPEST (kompromittáló elektromágneses kisugárzás elleni védelem) mérésére szolgáló stacionáris és mobil laboratóriumok üzemeltetése is.

c) Idetartozna a minősített adatok védelmét szolgáló fizikai eszközök (zárak, ajtók, páncélszekrények) minősítése.

(5) ellátja a központi közigazgatási szervek és a helyi önkormányzati közigazgatási szervek hitelesítő szolgáltató feladatát[2];

(6) üzemelteti az informatikai vészjelző és beavatkozó központot[3];

(7) az államtitokról és a szolgálati titokról szóló 1995. évi LXV. törvény hatálya alá tartozó minősített adatot (továbbiakban: minősített adat) kezelő informatikai rendszerek létesítését, működtetését és megszüntetését engedélyezi;

(8) ellátja a minősített adatot tartalmazó informatikai rendszerek informatikai biztonsági szempontból történő felügyeletét és ellenőrzését;

(9) engedélyezi és nyilvántartja a fokozott biztonságú, valamint minősített elektronikus aláírás hitelesítés-szolgáltatókat, az elektronikus aláírás, illetőleg időbélyegző előállításához használt aláíró eszközöket és egyéb elektronikus aláírási termékeket;

(10) biztosítja az állami irányítás alatt álló és a stratégiai feladatokat ellátó szervezeteknél az informatikai rendszerei biztonsági követelmények érvényesülésének ellenőrzését,

(11) biztosítja a közigazgatás, az állami irányítás alatt álló szervezetek, a stratégiai feladatokat ellátó szervezetek informatikai rendszerei szükségállapotban történő védelmére a megfelelő tervek kidolgozását;

(12) kivizsgáltatja a közigazgatás, az állami irányítás alatt álló szervezetek, a stratégiai feladatokat ellátó szervezetek informatikai rendszerei biztonságával kapcsolatos eseményeket;

(13) gondoskodik az informatikai rendszerek vagy eszközök biztonsági vizsgálatával, a minősített adatot tartalmazó és stratégiai jelentőségű informatikai rendszerek biztonságával kapcsolatos oktatások, a szükséges továbbképzések és vizsgáztatások lebonyolításáról;

(14) tevékenysége során együttműködik a Nemzeti Biztonsági Felügyelettel, a BM Titokvédelmi Osztállyal, az IH Országos Rejtjelfelügyelettel, a HM Információ- és Dokumentumvédelmi Főosztállyal;

---

[2] Az elektronikus aláírásról szóló törvényben az un. PKI felhasználása rejtjelzési célokra nincs szabályozva, de például a NATO elvárja, hogy a levelezés elektronikusan és rejtjelzetten történjen!

[3] Az informatikai vészjelző és beavatkozó központ szerepe kiemelt jelentőségű. Jelenleg sem előrejelző (riasztó), sem beavatkozó szervezet nincs hazánkban.

(15) tájékoztatja a Kormányt, az EU, a NATO, illetve a NYEU illetékes szervezeteit tevékenységéről;

(16) kapcsolatot tart az EU, a NATO, a NYEU és a tagállamok illetékes szervezeteivel;

(17) vezeti a tevékenységével kapcsolatos nyilvántartásokat, és ezeket az illetékesek számára hozzáférhető és folyamatosan elérhető módon közzéteszi.